What is claimed is:

1. A method of providing a secure transaction key, the method comprising:

a. providing a transaction key generator having an internal-key biometric input arrangement, for storing a password derived from the biometric input, and for generating a transaction code based on a transaction input, a biometric input, and the internal key;

b. deriving a personal key based on the internal key and a biometric input, and transferring the personal key to a server in a secure initialization session;

c. using the transaction key generator to derive a transaction code for each transaction that is communicated to the server at the time when transaction parameters are transmitted to the server;

d. at the server level, using the transaction parameters and the personal key to generate a reference that is compared with the transaction code to authenticate the transaction.

2. A method of providing a secure authentication code from a network client to a network server, the method comprising:

prompting a user to provide a biometric input;

decrypting an encrypted biometric token representative of a biometric input from an authorized user;

correlating the biometric input with the decrypted biometric token and, when the biometric input correlates to within a selected threshold of the decrypted biometric token, cryptographically transforming the biometric token to generate an authorization token;

processing the authorization token to generate an encrypted authorization code; and

forwarding the encrypted authorization code to the network server.

3. A method according to claim 2, wherein the biometric input is a spoken phrase, and the biometric token is a representation of the spoken phrase from an authorized user.

4. A method according to claim 2, wherein the biometric token is encrypted and decrypted with a cryptographic key representing selected bits of a larger Data Encryption Standard (DES) key.

5. A method according to claim 4, wherein cryptographically transforming the biometric token includes:

processing the biometric token with a first transforming key representing selected bits of the DES key to produce a first intermediate token;

processing the first intermediate token with a second transforming key representing selected bits of the DES key to produce a second intermediate token, the second transforming key being different from the first transforming key; and

processing the second intermediate token with the first transforming key to produce the authorization token.

6. A method according to claim 2, wherein correlating the biometric input with the decrypted biometric token includes adding reverb to the biometric input and the decrypted biometric token.